DOCUMENTO DE IDENTIFICAÇÃO ÚNICO: O CIDADÃO DIGITAL

Cláudio Kaipper Ceratti

2007

CLÁUDIO KAIPPER CERATTI

DOCUMENTO DE IDENTIFICAÇÃO ÚNICO: O CIDADÃO DIGITAL

Monografia apresentada para a obtenção do título de Especialista em Criptografia e Segurança em Redes no Curso de Pós-graduação Lato Sensu em Criptografia e Segurança em Redes da Universidade Federal Fluminense.

Orientador: Prof. Dr. Luiz Manoel Silva de Figueiredo

Niterói

2007

Ceratti, Cláudio Kaipper
DOCUMENTO DE IDENTIFICAÇÃO ÚNICO: O CIDADÃO DIGITAL / Cláudio Kaipper Ceratti–
Niterói, 2007.
41 f.: il., 30cm.
Trabalho Final de Curso (Especialização em Criptografia e Segurança de Redes) – Universidade Federal Fluminense, 2006.
1. Criptografia. 2. Documento de identidade. 3. Identificação presencial e remota. 4. Redes de computadores – Medidas de segurança – Tese I. Título.

CLÁUDIO KAIPPER CERATTI

DOCUMENTO DE IDENTIFICAÇÃO ÚNICO: O CIDADÃO DIGITAL

Monografia apresentada para a obtenção do título de Especialista em Criptografia e Segurança em Redes no Curso de Pós-graduação Lato Sensu em Criptografia e Segurança em Redes da Universidade Federal Fluminense.

BANCA EXAMINADORA

_____

Prof. Dr. **LUIZ MANOEL SILVA DE FIGUEIREDO** - (orientador).

_____

Prof. Dr. **MÁRIO OLIVERO**.....

_____

Profa. Dra. **NANCY CARDIM**.....

Aprovada em ____/____/_____.

RESUMO

Este trabalho apresenta a situação atual da utilização de documentos eletrônicos de identificação do cidadão em países europeus, e as perspectivas para a implantação de uma nova forma de identificação no Brasil.

Na Introdução, apresentamos um histórico da identificação como relação do indivíduo com a sociedade, e sua rápida evolução com o advento da Internet. Aí estão também os tópicos referentes à nossa Motivação para a elaboração deste trabalho, à Metodologia empregada, e aos Objetivos.

Na Seção 1, apresentamos uma visão da estrutura básica de identificação, resumos do conceito e evolução da criptografia, de ferramentas derivadas e complementares para seu uso, como a Infra-estrutura de Chaves Públicas, o suporte físico e lógico para a identificação do cidadão, e a integração de sistemas que se faz necessária para maximizar os benefícios das novas tecnologias.

Na Seção 2, apresentamos um resumo das experiências de alguns países europeus que já iniciaram esse processo.

Na Seção 3 apresentamos a situação atual do Brasil, em face de mudanças na tecnologia, mudanças de comportamento e conseqüentes mudanças legais que têm acontecido. Em particular, abordamos a promulgação da Lei 9454/97 e sua iminente regulamentação, a expansão das atividades do INI – Instituto Nacional de Identificação, e a regulamentação e implantação da Infra-estrutura de Chaves Públicas brasileira - ICP-Brasil, que ajudam a formar a base para uma mudança profunda na forma de identificar os cidadãos em nosso País.

Ao final, apresentamos nossas Conclusões.

SUMÁRIO

ÍNDICE DE FIGURAS

1. INTRODUÇÃO

> *"A identificação é o ato de vontade pelo qual o cidadão se dá a conhecer perante terceiros, como sujeito titular de direitos e deveres"*. [1]

Segundo o Dicionário Aurélio Buarque de Holanda Ferreira, "cidadania é a qualidade ou estado do cidadão", entendendo-se por cidadão "o indivíduo no gozo dos direitos civis e políticos de um Estado, ou no desempenho de seus deveres para com este" [2]. No sentido ateniense do termo, cidadania é o direito da pessoa em participar das decisões nos destinos da Cidade. Num sentido abrangente, o Direito do Cidadão é o Direito de Acesso.

Como protocolo de comunicação com o cidadão, o Estado instituiu a Identificação, com atos formais de Registro e respectiva emissão de Documentos, que terminaram se transformando em condição essencial para acesso à educação, ao emprego e à saúde, dentre outras coisas.

Esses documentos, tal como atualmente utilizados, supõem uma identificação presencial. No sistema atual de identificação brasileiro são emitidos documentos em papel, cujo modelo é padronizado em todo o território nacional (Decreto 89250, 1983) [3]. Apesar da padronização, tais documentos são emitidos em meio e formato ultrapassados, facilmente adulterável, não fornecendo garantias de não-repúdio.

De acordo com estatísticas fornecidas pela Polícia Civil do Distrito Federal (DEPO 2008), as ocorrências envolvendo o roubo/furto de documentos atingiram 113.615 boletins em 2007, com alta de 23,84% em relação a 2006. Este fato demonstra que a falta de mecanismos inteligentes que preservem a garantia de confiabilidade e integridade deste tipo de documento coloca em risco não só a boa reputação do cidadão, que pode ter seus dados copiados e utilizados para fins ilícitos, mas também toda uma cadeia de acreditação que se baseia em técnicas ultrapassadas para promover sua identificação e registro.

Com a multiplicação da capacidade de atendimento do Estado a determinados serviços utilizando meios eletrônicos, se torna imperiosa a revisão do conceito de documentação do cidadão, de forma que esse possa acessar remotamente informações pessoais e serviços, sem que se comprometam a Integridade e Confidencialidade dos seus dados, e seja assegurado o Não-Repúdio dos atos por ele praticados.

A fim de prover estas facilidades, a Criptografia – e as funcionalidades relacionadas ao uso de assinaturas eletrônicas e certificados digitais – vem sendo amplamente utilizada como mecanismo essencial para assegurar a confidencialidade e integridade de

mensagens e a autenticação de parceiros de transações eletrônicas. Como detalharemos mais adiante, a chamada criptografia assimétrica, associada a uma rede de acreditação denominada Infra-estrutura de Chaves Públicas tem facilitado essa tarefa.

O Governo Brasileiro vem buscando informatizar os serviços oferecidos à população, a fim de facilitar as relações entre o Estado e o cidadão, tornando-as mais ágeis, permitindo que fluam com maior liberdade, a fim de que o exercício da cidadania seja uma realidade palpável nessa relação entre ambas as partes. Exemplos disso são a criação dos portais E-Gov e Brasil, a consulta à situação fiscal junto à Receita Federal, consulta a serviços do INSS (PrevCidadão), consulta a saldos do FGTS. Até o momento porém, cada uma dessas consultas exige um diferente tipo de cadastramento prévio para fins de acesso, com a Receita Federal utilizando já uma forma dentro dos moldes padronizados e mundialmente adotados de identificação segura. Além disso, alguns bancos já utilizam essa modalidade de autenticação para os clientes de internet banking.

Com a instituição da Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil [4], e com a promulgação de Medidas Provisórias que apóiam a utilização de Certificados Digitais em todas as esferas do Governo e também pelo cidadão comum, buscou-se encontrar uma solução para estas questões, pois se determina que os documentos produzidos, emitidos ou recebidos por órgãos e empresas públicas por meio eletrônico têm o mesmo valor jurídico que os produzidos em papel ou em outro meio físico reconhecido legalmente, desde que assegurada a sua autenticidade, integridade e não-repúdio.

Paralelamente, após mais de dez anos da sanção da Lei 9454/97 [5], que determina a criação do Cadastro Nacional de Registro de Identificação Civil - onde cada cidadão brasileiro, nato ou naturalizado, será identificado por um número único de registro - se abriu no Brasil a oportunidade de iniciar o estudo de um novo modelo de documento de identidade, que contemple a extensão da autenticação presencial para a autenticação remota.

2. JUSTIFICATIVA

Do exposto acima, percebemos um movimento de caráter amplo na adoção de uma nova forma de comunicação dos cidadãos com as organizações e com o estado, e que demanda mudanças bastante grandes nesse protocolo de identificação. No caso brasileiro, a regulamentação da Lei 9454/97 e a posta em marcha do projeto RIC – Registro de Identidade Civil, tornam oportuna uma comparação de objetivos, métodos e técnicas propostas com as de países que já estão implementando essa solução, principalmente quanto a padrões adotados. Entendemos ainda que a sociedade deva discutir aspectos de privacidade e do eventual aumento do controle do cidadão pelo Estado, haja vista que a condução desse processo no Brasil está nas mãos das autoridades policiais.

Neste trabalho, serão abordadas as vantagens da transformação das atuais estruturas oficiais de identificação do cidadão para o modelo de Infra-estrutura de Chaves Públicas, e os problemas relacionados à mudança deste paradigma, tais como o custo envolvido; o retorno esperado, sob a ótica da eliminação de barreiras de tempo e lugar; as contradições de um país pobre, onde os serviços normalmente são para quem pode pagar por eles; as mudanças culturais decorrentes e a complementação de outras atividades informatizadas voltadas para a cidadania, como o Voto Eletrônico.

3. METODOLOGIA

Para a confecção deste trabalho, foram adotadas as seguintes técnicas:

- Entrevistas;
- Consulta em livros;

. Participação em fórums e seminários específicos sobre o assunto;

- Consultas realizadas na internet, em páginas tidas como confiáveis pela comunidade, tais como: centros de pesquisa, páginas relacionadas ao Governo Federal, buscadores e afins.

4. OBJETIVOS

O objetivo deste trabalho é estudar os possíveis usos dos Certificados Digitais no exercício da Cidadania, principalmente aqueles relacionados ao estabelecimento da confiança na identificação do indivíduo perante a sociedade, através de mecanismos seguros e modernos, capazes de garantir duas premissas de alta relevância: A autenticidade e o não-repúdio de sua identificação. Buscaremos propostas para questões tais como:

– Transformação das atuais estruturas oficiais de identificação do cidadão (Ex.: Institutos de Identificação) para o modelo da Infra-estrutura de Chaves Públicas: Autoridades Certificadoras (AC) e Autoridades de Registro (AR).

- A inércia da mudança.

– O custo envolvido.

– O retorno esperado, sob a ótica da eliminação de barreiras de tempo e lugar.

– Paralelo com outras soluções, bancária por exemplo.

– Mudanças culturais decorrentes, como a redução ou mesmo eliminação do contato direto do cidadão com os agentes do Estado, o aumento da responsabilidade pelo mau uso das ferramentas, o eventual aumento do controle do indivíduo pelo Estado.

– O possível agravamento de uma nova modalidade de crime, envolvendo fraudes e roubo de identidades.

- Complementação de outras atividades informatizadas voltadas para a cidadania, como o Voto Eletrônico.

DESENVOLVIMENTO

1. SEÇÃO 1

1.1. COMUNICAÇÃO SEGURA

Com a massificação do uso da WWW (World Wide Web), que no jargão popular se confunde com a Internet, diversos serviços foram sendo colocados à disposição dos cidadãos, como transações bancárias (Internet banking), transações comerciais (e-commerce, ex.: compras pela internet), trocas de mensagens (email), transações com o Governo (e-Gov, ex.: declaração do Imposto de Renda), como forma de facilitar o uso, reduzir tempos, custos e distâncias, aumentar a capacidade e os horários de atendimento. A maioria desses serviços exige uma troca de dados sensíveis (sigilosos e/ou reservados) entre as partes que se comunicam, o que leva à necessidade do estabelecimento de uma relação de confiança entre elas, ou seja, o prestador de serviços necessita saber com segurança se quem está fazendo um acesso e solicitando esses serviços é mesmo quem diz ser; o tomador do serviço, por sua vez, necessita saber se o computador remoto que está acessando pertence realmente ao prestador de serviços, e ambos têm que se assegurar que a conexão estabelecida esteja livre da interferência de terceiros que possam capturar ou adulterar as informações que por ela transitem. Além disso, em várias situações é fundamental que nenhuma das partes venha, posteriormente, repudiar como falsa uma transação eventualmente resultante. Esses problemas precedem a internet, e têm sido resolvidos, ao longo da história da humanidade, com o uso de técnicas de criptografia aplicada e tecnologias associadas, tais como protocolos seguros de comunicação e a certificação digital. Dado que a ferramenta básica do usuário para acesso é o navegador (ex. Firefox, Internet Explorer, KDE), é óbvio que este também teve que incorporar essas técnicas.

1.2. CRIPTOGRAFIA

O termo Criptografia surgiu da fusão das palavras gregas “Kryptós” e “gráphein”, que significam “oculto” e “escrever”, respectivamente. Na prática, aborda conceitos e técnicas cujo objetivo é evitar o acesso de pessoas não-autorizadas a informações sensíveis, a fim de que sua confidencialidade seja mantida. Um texto criptografado é o resultado de um texto original, submetido a um algoritmo de cifragem e uma chave. A decifragem se faz pela

operação inversa, o que obriga a que tanto o algoritmo quanto a chave sejam do conhecimento de todas as partes legitimamente interessadas.

O uso de criptografia para manter mensagens ocultas vem de tempos remotos, onde os métodos, muitas vezes artesanais, foram substituídos por modernos e robustos algoritmos, cuja finalidade é dificultar ao máximo a quebra do seu segredo e, assim, prover a propriedade da confidencialidade, qualidade altamente necessária nos tempos da "Sociedade da Informação", onde diversas tecnologias estão difundidas e a busca por vulnerabilidades em sistemas de proteção é intensa.

Para o usuário final, atualmente a Criptografia tem sido essencial para assegurar a confidencialidade das transações via *Internet Banking* e em transações de comércio eletrônico. Já pelo lado das empresas, é necessário prover mecanismos eficazes na proteção da base de dados de seus usuários, a fim de evitar que números de cartões de crédito e outros dados pessoais sejam acessados por pessoas não-autorizadas. Assim, a criptografia se tornou não somente ferramenta imprescindível para a proteção de informações vitais ao negócio de uma empresa, mas também o fator diferencial no relacionamento com seus clientes.

Os principais obstáculos no uso da criptografia têm sido, ao longo do tempo, o desenvolvimento de algoritmos seguros, a definição de qual algoritmo a utilizar na comunicação cifrada entre as partes interessadas, a guarda e distribuição das respectivas chaves e o tempo necessário para cifrar e decifrar as mensagens. Particularmente no caso das chaves, sua captura por um oponente compromete todo o processo, ainda mais quando os algoritmos utilizados são conhecidos, tornando crucial sua guarda segura e distribuição, eventualmente para um número elevado e geograficamente disperso de participantes. Atualmente são utilizadas duas modalidades principais de algoritmos criptográficos, denominados de criptografia simétrica e assimétrica:

1.2.1. Simétrica

Nesta modalidade, a chave utilizada para cifrar uma mensagem é a mesma utilizada para decifrá-la. Apesar do algoritmo de criptografia executar a tarefa com certa rapidez, seu maior problema consiste na distribuição e na guarda da chave secreta, já que esta deve ser divulgada através de meio seguro, a fim de manter a confidencialidade das comunicações. Enquanto a chave permanecer secreta, apenas o transmissor e o receptor da mensagem podem ter acesso ao seu conteúdo.

Dentre os principais algoritmos, podemos citar o DES, 3DES e o Blowfish.

1.2.2. Assimétrica

É baseada no conceito de par de chaves: uma chave privada e uma chave pública, onde uma mensagem cifrada com uma das chaves do par só pode ser decifrada com a outra chave correspondente. A fim de proteger o sigilo da comunicação, a chave privada deve ser mantida secreta, enquanto que a chave pública pode ser disponibilizada a quem de interesse.

Apesar da facilidade na troca de chaves, os algoritmos de criptografia assimétrica são mais lentos, pois requerem elevado poder de processamento da máquina durante a cifragem dos dados. Por este motivo, normalmente são utilizadas formas híbridas de criptografia onde, por exemplo, a criptografia de chave pública forma o canal seguro para a distribuição das chaves simétricas, que por sua vez é mais rápida que o uso do par de chaves da criptografia assimétrica.

Dentre os principais algoritmos, podemos citar o RSA e o Diffie-Hellman

1.2.3. Assinatura Digital

É um mecanismo criado para atribuir confiabilidade a um documento eletrônico, pois possibilita a autenticação da identidade da assinatura, eliminando a possibilidade de que o autor venha a negá-la.

A assinatura digital resulta da combinação de uma operação matemática onde é criado um resumo dos dados do documento utilizando uma função hash (através dos algoritmos MD5, SHA-1, SHA-256, por exemplo), e da consequente cifragem da mensagem com a chave privada de seu emissor. Pela característica pessoal e confidencial da chave privada, considera-se a assinatura digital como um meio legalmente aceito para que pessoas possam assinar documentos eletrônicos com a mesma validade jurídica de sua assinatura de "próprio punho". Deve ser autêntica (a identidade do assinante deve ser garantida), à prova de fraude (a assinatura não pode ser falsificada), não reusável (deve fazer parte de um documento somente, e não pode ser transferida para outro), inalterável (qualquer alteração no documento invalida a assinatura), e irrevogável (o assinante não pode retirar a assinatura do documento).

1.3. INFRA-ESTRUTURA DE CHAVES PÚBLICAS

Como mencionado anteriormente, a gerência das chaves, aí compreendidas sua geração, distribuição e guarda, tem sido um dos principais segredos a zelar no uso da criptografia. Nesse conceito de criptografia assimétrica, como vimos, posso publicar minha chave pública para que outras pessoas, mesmo sem prévio contato comigo, possam me mandar mensagens criptografadas. Mas como impedir que um terceiro mal-intencionado

publique uma chave como sendo minha para, posteriormente, receber as mensagens que outras pessoas estão supostamente enviando para mim? Para facilitar essa troca e agregar confiabilidade às chaves criou-se o conceito de infra-estrutura de chaves públicas (em inglês PKI: Public Key Infrastructure), que consiste num conjunto de hardware (e.g., smart cards e servidores), software (cliente, servidor), contratos legais e garantias, e procedimentos operacionais, voltados ao armazenamento de chaves públicas. Publicar minha chave através da PKI, que inicialmente se assegura de minha identidade, possibilita que ela certifique sua autenticidade. Sua estrutura está baseada em uma cadeia de autoridades certificadoras, formada por uma Autoridade Certificadora Raiz (AC-Raiz), Autoridades Certificadoras (AC), eAutoridades Registradoras (AR) e um Comitê Gestor. Seu funcionamento deve obedecer a uma Política de Certificados e a uma Declaração de Práticas de Certificação. Na Seção 3, quando falarmos da ICP-Brasil, apresentaremos um esquema detalhado dessa hierarquia e de seu funcionamento.

1.3.1. Autoridade Certificadora Raiz – AC-Raiz

Hierarquicamente, é a AC-Raiz quem detém o certificado de nível mais alto dentro de uma estrutura de Chaves Públicas, servindo como referência na verificação da validade da cadeia. Seu certificado contém a chave pública correspondente à chave privada da AC Raiz, utilizada para assinar o seu próprio certificado e os das Autoridades Certificadoras localizadas no nível logo abaixo.

1.3.2. Autoridades Certificadoras – ACs

Também conhecidas como “Terceiro Confiável”, são entidades credenciadas que emitem certificados digitais vinculando pares de chaves criptográficas a um determinado titular. Têm o poder de emitir, expedir, distribuir, revogar e gerenciar os certificados, devendo disponibilizar publicamente listas contendo informações de certificados revogados (LCRs) para que possa ser verificada a validade de um determinado certificado.

1.3.3. Autoridades de Registro – ARs

São entidades operacionalmente vinculadas a uma AC Habilitada responsáveis pelo processo final na cadeia de Certificação Digital, atendendo os interessados em adquirir certificados e coletando os documentos para encaminhá-los às ACs, responsáveis pela emissão do certificado.

1.3.4. Software:

É relativamente fácil para uma organização montar sua própria Autoridade Certificadora, com o que pode autenticar acessos e comunicações internas. O Windows 2000 Server e Windows 2003 Server contêm software de AC integrado no Active Directory, sem necessidade de licenciamento adicional. Linux suporta OpenSSL e Open CA, que são duas soluções de código aberto existentes. O pacote Entrust Authority é bastante popular entre as soluções pagas.

1.4. OS CERTIFICADOS DIGITAIS

O CERTIFICADO DIGITAL é um arquivo eletrônico que permite verificar se uma chave pública pertence a uma determinada identidade, seja essa uma pessoa ou organização. Para isso, ele tem uma assinatura digital de um "terceiro confiável" que atesta que aquela identidade está associada à chave: De uma Autoridade Certificadora, se num esquema de ICP como descrito acima ou, se num esquema conhecido como "web of trust", de alguém em quem podemos acreditar ou não.

Seu uso vem trazer maior segurança às transações eletrônicas, garantindo a essas transações Autenticidade, Integridade e Não Repúdio. Essas três características são também conferidas aos documentos assinados com um certificado digital. A Autenticidade garante que o autor é a pessoa identificada no certificado utilizado na assinatura. A Integridade garante que o documento não foi alterado após o envio. O Não Repúdio garante que o autor não possa contestar sua validade negando a autoria, após a assinatura. O Certificado Digital também pode ser utilizado para login seguro na rede, para estabelecer conexões seguras entre equipamentos, assinatura e criptografia de correio-eletrônico e criptografia de arquivos. Normalmente seguem o padrão ITU X.509, referenciado pela RFC 2459.

Por conter os dados de seu titular, chave pública, nome e assinatura da Autoridade Certificadora que o emitiu, funciona como uma carteira de identidade virtual que permite a identificação segura de uma mensagem ou transação em uma rede de computadores. Pode ser armazenado em um meio magnético ou ótico [18].

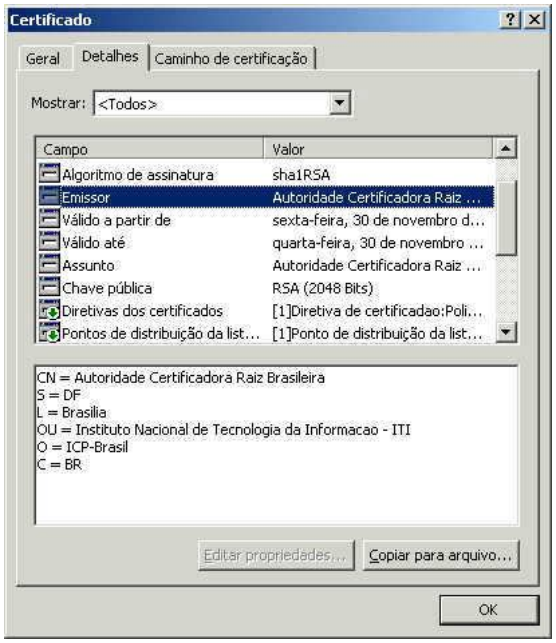

Figura 1: Certificado emitido pela AC Raiz

1.5. DOCUMENTO DE IDENTIFICAÇÃO ÚNICO – O SUPORTE

Pensando em um mundo globalizado onde a Internet reduziu drasticamente os conceitos de distância e disponibilidade de serviços, é possível encontrar diversas aplicações disponíveis para a utilização de certificados digitais.

Vários países no mundo já vêm modernizando a forma de registro do cidadão, adotando soluções que visam promover a Identificação de modo seguro e definitivo. A implantação deste novo modelo é alicerçada por intenso estudo que busca entender o panorama de sua aplicação e os impactos que implicam na mudança do paradigma atual, indo desde o modo de solicitação até a aceitação e reconhecimento da solução pelo cidadão.

A evolução tecnológica e o conseqüente aperfeiçoamento dos processos de produção têm viabilizado uma solução versátil, confiável e acessível para a questão do documento seguro, com características de funcionalidade integradoras, e que alguns países estabelecem como sendo único: O Smart Card, ou Cartão Inteligente, um cartão feito com material plástico, semelhante a um cartão de crédito, com um microchip embutido na superfície, também conhecido como ICC (Integrated Circuit Card - Cartão com Circuitos

Integrados). Além da identificação visual, os dados nele gravados podem ser acessados por contato físico, ou seja, através da inserção do cartão em uma leitora específica. Esses cartões são utilizados na Europa desde o início dos anos 90, e têm evoluído continuamente. Uma das maiores novidades nesse cartão é a utilização de materiais como o policarbonato, associado a um processo de produção que torna o documento impossível de adulterar por meios físicos e químicos, sendo o principal item de segurança física. Outra é a capacidade de processamento e de armazenamento do chip de contato, com vários dados, inclusive biométricos - notadamente as impressões digitais - e que assegura a segurança lógica.

Um Smart Card Microprocessado possui os principais elementos de um computador, como uma CPU (Central Processing Unit), um sistema de memórias e barramentos de entrada e saída. Um sistema operacional, gravado no cartão, permite que uma comunicação em alto nível possa ser estabelecida com a leitora a que está conectado.

Os cartões devem atender às especificações da ISO (International Standards Organization), eventualmente associada a outras organizações, como a IEC (International Electrotechnical Commission). Exemplos dessas normas são a ISO/IEC 7810 e a ISO/IEC 7816. Algumas das principais características dos Smart Cards com microprocessador são (Gemalto, 2008):

- Capacidade de Processamento -. Os cartões mais modernos utilizam um micro-controlador RISC de 32-bits rodando a um clock de 25 a 32 MHz. As suas instruções manipulam também os endereçamentos de memória e dos registradores e operações de entrada e saída. Alguns fabricantes implantam instruções próprias para um uso específico. Pode haver também um co-processador para a criptografia: Um processo de decriptação RSA 1024 bits, por exemplo, pode demorar até 10 segundos.
- Capacidade de Armazenamento - O Smart Card Microprocessado possui 3 tipos de memórias: ROM (Read-Only Memory), EEPROM (Electrically Erasable Programmable Read-Only Memory) e uma pequena quantidade de RAM (Random Access Memory). A ROM é onde o sistema operacional do Smart Card é armazenado e não pode ser alterada. A RAM é usada tanto pela aplicação quanto por rotinas operacionais. As memórias mais usadas nos Smart Cards são as EEPROM (Electrically Erasable Programmable Read-Only Memory) que possuem capacidade de 8 Kbit a 128 Kbit. (1 Kbit armazena algo em torno de 128 caracteres, o equivalente a uma frase de texto. Entretanto, com as modernas técnicas de compressão, a quantidade de

informação armazenada em um Smart Card pode ser bem maior). É na EEPROM que são armazenados os dados da aplicação, isto é, ela pode ser lida e escrita por aplicativos. Os dados presentes nessa memória podem permanecer, se não sobrescritos, por até 10 anos. Entretanto, a EEPROM possui 2 inconvenientes:

- Lentidão: Leva de 3 a 10 ms para se escrever nessa memória;
- Número de regravações: Pode chegar a no máximo 100.000 gravações.

- Correção de Erro - O Sistema Operacional do Chip (COS - Current Chip Operating Systems) executa seu próprio algoritmo de correção de erro.
- Custo - A média de preço de um cartão microprocessado é de US$ 3,79. O custo aumenta à medida que maior capacidade de armazenagem e de processamento são acrescentados ao chip e esse custo diminui a medida que o volume de produção aumenta.
- Confiabilidade – Os fornecedores garantem 10.000 ciclos de leitura/escrita. As normas ISO determinam uma bateria de testes que abrange: testes de torção, de flexibilidade, de desgaste, de concentração de carga, temperatura, umidade, eletricidade estática, ataque químico, ultra-violeta, raio X e testes de campo magnético.
- Segurança - Smart cards são altamente seguros. As informações armazenadas no chip são difíceis de serem copiadas ou alteradas, e não podem ser facilmente clonados. O microprocessador e o co-processador do chip suportam criptografia, autenticação e assinatura digital para não-repúdio. Alguns dos padrões exigidos são o EAL – Evaluation Assurance Level e o EMV – Europay Mastercard Visa (Ver Seção 5, Principais Padrões).

Outras características da arquitetura do Smart Card: O canal de entrada e saída do cartão é serial e unidirecional. Isto significa que os bits passam um a um em um único sentido de fluxo por vez. O hardware do Smart Card permite velocidades de até 115.200 bps.

A comunicação entre o cartão e o software de aplicação é do tipo mestre (software) e escravo (cartão). O software envia comandos ao cartão e espera por uma resposta. O cartão nunca envia dados ao software exceto em resposta a um comando. Ressalte-se que o cartão não possui baterias, sendo a alimentação elétrica feita pela leitora, quando de sua inserção.

Os cartões com a tecnologia Java (Java Cards) [6] executam aplicativos escritos nessa linguagem, possuindo os conceitos de máquina virtual que a plataforma Java exige (Sun

Microsystems, 2007). Essa tecnologia proporciona um ambiente seguro para as informações sensíveis, que ficam armazenadas no cartão junto com a sua respectiva aplicação. Há um firewall interno que isola as distintas aplicações, verificando e restringindo o acesso aos dados. Há também suporte a vários algoritmos criptográficos.

Os sistemas operacionais dos Smart Cards suportam dois tipos de transferência: por caractere ou por bloco. A transferência por caractere ocorre quando os dados são transferidos caractere a caractere até formar uma palavra. Já na transferência por bloco, são transmitidos quadros inteiros por vez, o que faz deste tipo de transferência mais complexo que o outro.

O processo de manufatura de um Smart Card compreende 8 etapas distintas:

1. Fabricação de milhares de chips em uma única pastilha de silício (wafer). Cada chip tem a forma de um quadrado de aproximadamente 5 mm de lado (25 mm2 de área, portanto). Esse modelo de chip é repetido até preencher toda a pastilha de silício (totalizando de 3000 a 4000 unidades por pastilha), num processo a vácuo, onde são depositados materiais extremamente puros no substrato de silício.
2. Empacotamento dos chips individuais para inserção dentro do cartão. Quando a pastilha está completa, cada chip é testado para verificar se está operacional. Cada chip aprovado é identificado através de uma marca física antes de a pastilha ser particionada. Uma vez que isto acontece, o chip é preso a uma lâmina de contatos, que possui fios de baixíssima bitola que conectam os terminais do chip a regiões específicas da lâmina. O resultado dessa união é chamado tecnicamente de módulo.
3. Fabricação do cartão. O cartão em si é feito em PC (PolyCarbonate) ou em PVC (PolyVinyl Choride) ou em ABS (Acrylonitrile Butadiene Styrene). Em PVC é possível criar formas em alto-relevo, porém este material não é reciclável; o ABS não é modelável em alto-relevo mas é reciclável. O material do cartão é produzido em larga escala e em produções massivas para um determinado cliente, pode-se imprimir algo na superfície, como por exemplo logotipos. Nos cartões em policarbonato objetos deste estudo, são utilizadas várias lâminas do material, cada uma com tratamento distinto.
5. Pré-personalização. A maioria das aplicações Smart Card requerem que certos programas ou arquivos sejam instalados em cada cartão, antes que o mesmo seja personalizado e entregue ao usuário. Isso é feito nesta etapa, na qual a

preparação do software do cartão é feita através do conector de I/O na superfície do cartão. Eventualmente deve ser executada uma fase para o estabelecimento das chaves criptográficas e geração do certificado digital.

6. Personalização. Este processo envolve a gravação de informações como nomes e números relacionados ao usuário. Isto usualmente também envolve a escrita do PIN (Personal Identification Number) na memória, número que identifica o usuário com o cartão. A personalização envolve ainda a manipulação física do cartão; figuras e informações como nome e endereço podem ser impressas em sua superfície. A impressão também pode ser feita em alto-relevo.
7. Impressão no cartão. Esta etapa envolve a impressão gráfica e textual no Smart Card, envolvendo símbolos, logotipos, a foto, nome e demais dados da pessoa portadora. Também são impressos hologramas e outros artifícios de segurança para evitar fraudes. Dependendo da informação a ser armazenada, vários processos de impressão podem ser empregados. Para cartões que possuem o mesmo design gráfico, como cartões telefônicos, a estampa pode ser feita antes da inserção do circuito integrado no molde; neste caso, a impressão é feita na manta plástica, antes de se extrair o molde. Nos cartões em policarbonato, como mencionamos anteriormente, os dados são gravados através de feixes de laser que perfuram as várias lâminas do material, num processo de fusão denominado "gravação a laser" (http://en.wikipedia.org/wiki/Laser_engraving).
8. Inicialização do programa contido no cartão. Finalmente são executados os programas que rodam no próprio cartão (se microprocessado), e, então, o Smart Card está disponível ao usuário final.

As características mostradas nas figuras seguintes são do Cartão do Cidadão implantado em Portugal (Gemalto, 2008):

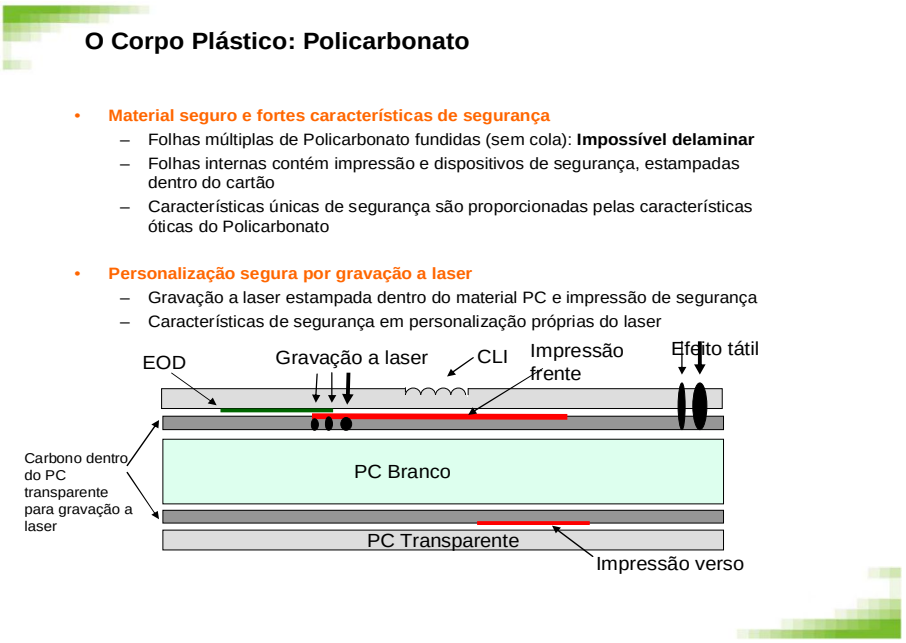

Figura 2: Estrutura do smart card utilizado em Portugal.

Como já citado, a tentativa de adulterar o cartão resulta em dano permanente e irrecuperável.

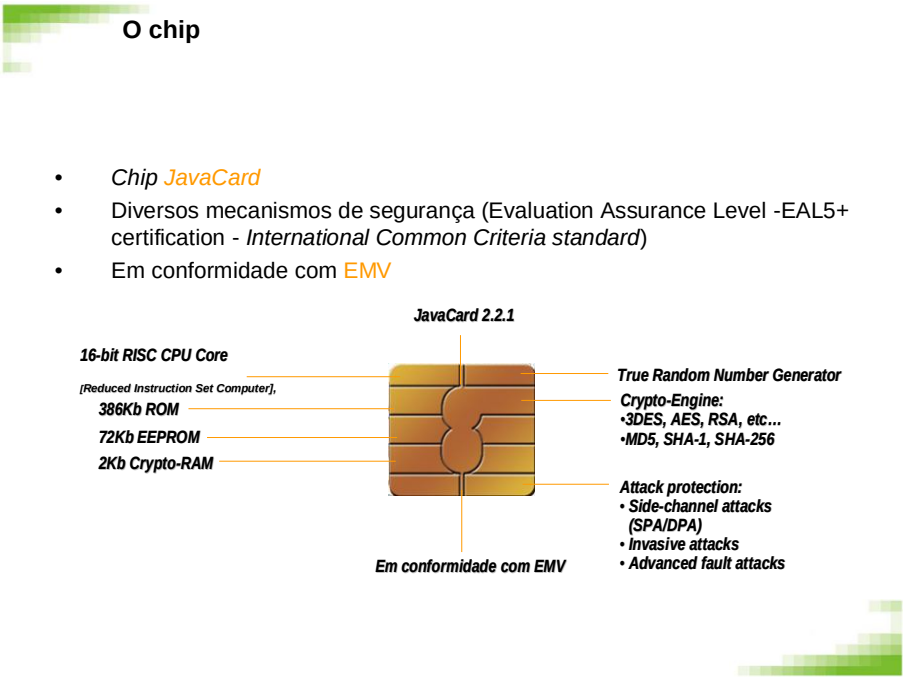

Figura 3: Características do chip do smart card utilizado em Portugal.

As características e padrões implantados impedem que dados sensíveis sejam exportados e, como mencionado anteriormente, permitem segregar aplicações dentro do chip, impedindo que uma organização tenha acesso não autorizado a dados de outra organização.

O chip: Aplicações e dados

- Aplicações:
  - IAS - aplicação responsável pelas operações de autenticação e assinatura electrônica
  - EMV-CAP - aplicação responsável pela geração de *one-time-passwords* por canais alternativos (e.g., telefone)
  - Match-on-Card - aplicação responsável pela verificação biométrica de impressões digitais

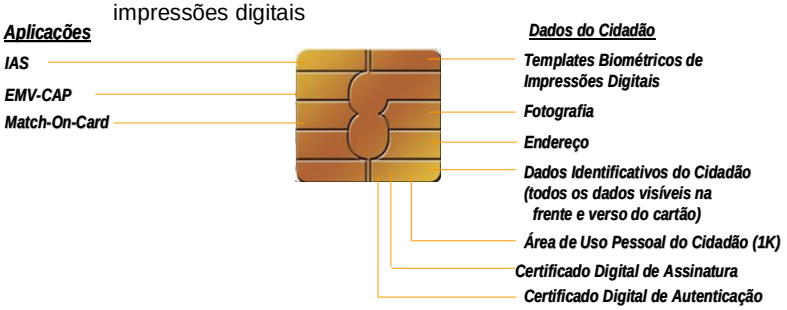

Figura 4: Aplicações e dados gravados no smart card utilizado em Portugal.

Layout: Frente

- Formato ID-1 em policarbonato com diversas características de segurança (verificáveis em 3 níveis)
- A frente do cartão do cidadão possui informações pessoais de identificação do titular do documento

Figura 5: Frente do smart card utilizado em Portugal.

Layout: Verso

- Informações específicas das entidades (Receita Federal, Previdência Social, Saúde, etc…)
- Área de Leitura a Máquina (Machine Readable Zone - MRZ)

Figura 6: Verso do smart card utilizado em Portugal.

1.6. A INTEROPERABILIDADE

Interoperabilidade é a capacidade de uma organização ou sistema de se comunicar e trabalhar, da forma mais transparente possível, com outra organização ou sistema, semelhante ou não. Para isso é necessário estabelecimento de uma relação de confiança e um diálogo eletrônico seguro entre duas estruturas, no mesmo ou em diferentes países. Isso envolve aspectos legais, organizacionais e semânticos, assim como arcabouços de confiança, segurança e técnica. No Brasil há vários dados submetidos por lei a sigilo, tais como os bancários e fiscais. Como exemplo, quando da implementação da CPMF houve resistência do Banco Central em fornecer seus dados à Receita Federal: Essa os queria para rastrear eventuais fraudes no imposto de renda.

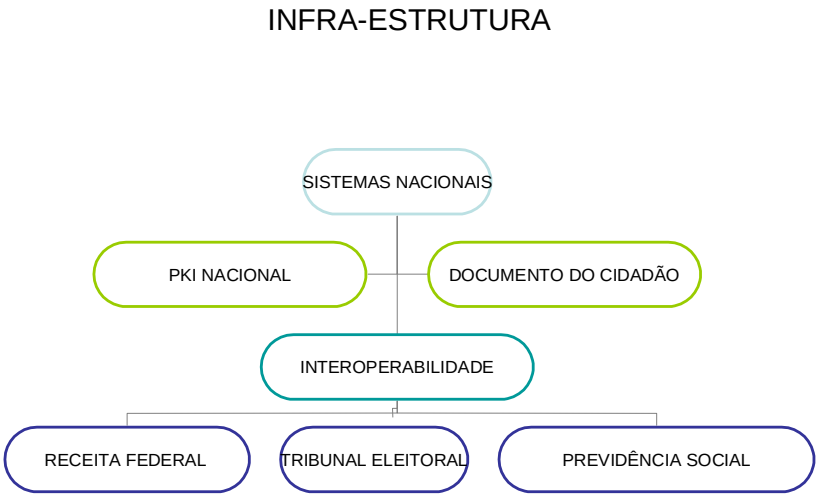

Figura 7: Exemplo da interoperabilidade entre sistemas nacionais acessados pelo cidadão

2. SEÇÃO 2 - EXPERIÊNCIAS DE IMPLANTAÇÃO

No inicio dos anos 2000, vários países europeus iniciaram uma transposição simples e direta de alguns dos serviços públicos para a modalidade on-line. Esses projetos eram, na sua maioria, centrados na tecnologia, ou seja, se buscava modernização e disponibilidade, com a satisfação dos cidadãos em segundo plano. Atualmente, muitos desses projetos estão já operacionais, e se inicia uma segunda fase, a de criar serviços on-line "inteligentes", agora centrados no cidadão. De toda forma, a implantação de uma nova forma de identificação do cidadão-usuário foi o ponto de partida para isso. Apresentamos a seguir algumas dessas experiências:

2.1. PORTUGAL

Portugal iniciou a implantação piloto de seu cartão em 2007 [7] [8], projeto a cargo da AMA – Agência para a Modernização Administrativa, uma instituição do Governo português. Tem como objetivo básico ser um documento físico que permita identificar o cidadão presencialmente, e um documento digital que permita identificação remota e assinatura eletrônica. Tem como objetivos paralelos aumentar o número de usuários de internet, aumentar as transações de eCommerce, e aumentar o uso de banda larga nas comunicações. O cartão é obrigatório para todos os cidadãos, mas há um cronograma de implantação por região do país. Vai substitui 5 outros documentos: Identidade, Previdência Social, Saúde, Receita Federal e Eleitor. Tem validade de 5 (cinco) anos. Sua emissão é centralizada, mas a solicitação e captura de informações é descentralizada. Tem como conteúdo biométrico impressões digitais e pontos da face. Um dos objetivos é ambicioso: Equipar policiais nas ruas com terminais de verificação, conforme figura a seguir.

Portugal possui uma ICP nacional denominada Entidade de Certificação Eletrônica do Estado - Infra-Estrutura de Chaves Públicas (ECEE).

SITUAÇÃO EM 2007 [9]:	CIDADÃOS	EMPRESAS
Porcentagem com acesso à Internet	35%	77%
Acesso aos serviços públicos pela Internet	14%	53%
Número de cartões emitidos	25.000	

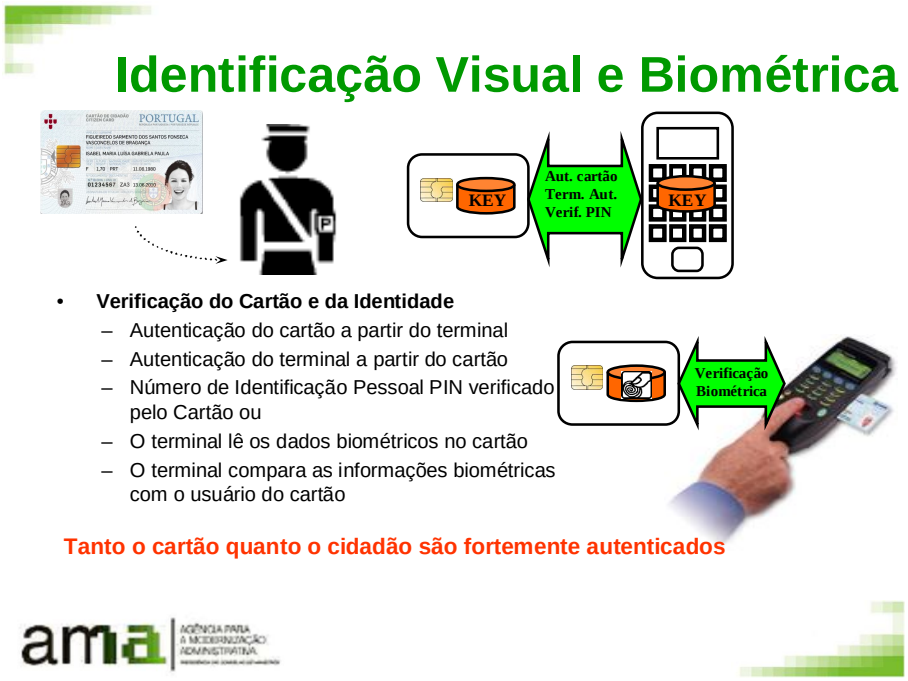

Figura 8: Terminal de verificação do cartão português. Fonte: AMA http://www.ama.pt/

2.2. ESPANHA

Um Decreto Real regula a expedição do DNIe (Documento Nacional de Identidade eletrônico) e seus certificados de firma eletrônica [8]. A ICP que dá suporte ao DNIe tem uma AC raiz e três ACs subordinadas, a cargo da DGP (Direção Geral da Policia - Ministério do Interior). A DGP atua também como Autoridade de Aprovação de Políticas, responsável por aprovar a Declaração de Práticas de Certificação, assim como suas modificações.

São utilizados o algoritmo RSA, e hash SHA-1 (para interoperabilidade com sistemas legados) e SHA-256. A AC raiz só emite certificados de chave pública para si mesma e suas subordinadas, e sua chave é de 4096 bits. Essas a sua vez emitem certificados de chave pública aos cidadãos, que se guardam no cartão criptográfico que constitui o DNIe junto com suas chaves privadas associadas. O tamanho dessas chaves é de 2048 bits. O acesso ao cartão está protegido por uma chave pessoal (PIN) que só o cidadão conhece. As chaves privadas permanecem no cartão e não podem ser exportadas em nenhum formato. O cartão tem dois certificados, um para autenticação e outro para assinatura eletrônica. A validade do documento varia conforme a idade do cidadão, variando de 5 anos a permanente, mas os certificados têm validade de 2,5 anos apenas. A troca ou renovação do cartão ou do

certificado implica em mudança de chaves. Estão gravadas no cartão as impressões digitais, imagem facial, e assinatura digitalizada.

2.3. BÉLGICA

Na Bélgica, existe desde Setembro de 2004 um cartão de identidade eletrônico, com as mesmas funções que os cartões de identidade tradicionais, cujo objetivo é ser o único instrumento para o acesso a eServices Públicos ou Privados. O cartão inclui suporte a assinatura digital, e pode também ser usado como documento oficial de viagem para os países do "Espaço Schengen" (quase todos os países da União Européia, mais Islândia, Noruega e Suíça). A Bélgica possui uma ICP nacional, prestando serviços de autenticação para os cidadãos, empresas e setor público. O Ministério para os Assuntos Internos funciona como a única Autoridade Certificadora (AC), sendo responsável pela gestão dos certificados durante o seu ciclo de vida, incluindo entre outros a sua emissão, suspensão, revogação, renovação e verificação de estado. Os municípios belgas são responsáveis por verificar a identidade do cidadão no processo de registro, funcionando como Autoridades Registradoras (AR), usando a base de dados do Registro Nacional e funcionando também como pontos de entrega. Estas entidades enviam todos os dados necessários para a geração ou revogação dos certificados à AC. [7] [8]

O cartão é obrigatório para todos os cidadãos e residentes com mais de 12 anos. È também de porte obrigatório. Sua obtenção e utilização são gratuitas. No chip estão gravados além dos dados impressos no cartão, o endereço do portador. Estão gravados também certificados para autenticação e assinatura digital com chave RSA de 1024 bits e hash SHA-1, e um certificado específico pertencente à AC, com chave de 2048 bits, que existe para controle do cartão, não permitindo acesso aos dados do cidadão. Apesar disso, há polêmica sobre a privacidade desses dados, tendo sido demonstrado que a proteção é falha (Gallo e Ávila, 2007) [8].

SITUAÇÃO EM 2007 [9]:	CIDADÃOS	EMPRESAS
Porcentagem com acesso à Internet	54%	96%
Acesso aos serviços públicos pela Internet	25,6%	43%
Número de cartões emitidos	5.000.000	

2.4. ÁUSTRIA

No caso da Áustria, não foi criado um cartão único do cidadão, mas sim um conceito [7] denominado Austrian Citizen Card, que define os requisitos necessários para a execução de procedimentos administrativos eletrônicos de forma segura, pelo que os cidadãos podem usar um cartão qualquer, desde que as entidades emissoras cumpram esses requisitos, sendo os mais importantes a assinatura e a identificação eletrônica. Esse "cartão-conceito" permite então ao cidadão acessar determinados serviços da Administração Pública. Assim, é um documento não totalmente padronizado, com exigências mínimas: pode ser requisitado por qualquer cidadão residente no país. Não substituiu quaisquer dos documentos previamente existentes.

Diferente dos demais países, a Áustria implantou um cadastro central com número único para identificar seus cidadãos e residentes. Esse cadastro deverá conter também seus respectivos endereços e senha (PIN) do cartão. Apesar disso, a utilização do cartão não é obrigatória

Interessante nesse caso foi o acordo que o governo austríaco fez com os bancos do país, que permitiu que os cartões bancários fossem aceitos pelo sistema, dando a essas instituições, de fato, o papel de Autoridades Registradoras. Dos cartões já disponíveis ou que serão brevemente disponibilizados, com base neste conceito, destacam-se os seguintes:

- Cartão "e-card" de Seguro de Saúde;
- Cartões bancários e MultiBanco com assinaturas eletrônicas;
- Documento de identidade com chip;
- Cartões emitidos por vários organismos públicos (ex.: notários).

SITUAÇÃO EM 2007 [9]:	CIDADÃOS	EMPRESAS
Porcentagem com acesso à Internet	52 %	94%
Acesso aos serviços públicos pela Internet	28%	76%
Número de cartões emitidos	9.000.000	

2.5. ESTÓNIA

O Cartão do Cidadão da Estónia destina-se a todos os cidadãos estonianos e a estrangeiros residentes há mais de um ano, possuidores de autorização de residência e com mais de 15 anos de idade. A utilização (porte) do cartão é obrigatória para todos. A autoridade emissora do certificado é formada por dois bancos e duas operadoras de telecomunicações

privadas. A personalização é feita por outra empresa privada, e entregue nas agências dos bancos mencionados. O cartão tem dois certificados, com senhas (PIN) diferentes: Um para autenticação e cifragem, e outro para assinatura digital, com chave RSA de 1024 bits e hash SHA-1. Esses certificados têm validade por 1100 dias.

SITUAÇÃO EM 2007 [9]:	CIDADÃOS	EMPRESAS
Porcentagem com acesso à Internet	46 %	90%
Acesso aos serviços públicos pela Internet	26,6%	66%
Número de cartões emitidos	1.300.000	

A Estônia foi o primeiro país do mundo a oferecer a opção de voto pela Internet: em Março de 2007, 30.000 eleitores votaram nas eleições gerais [9].

3. SEÇÃO 3 - BRASIL

3.1. LEI 9454/97

Conforme citado, a Lei 9454/97 que em seu artigo 1º determina que "*É instituído o número único de Registro de Identidade Civil, pelo qual cada cidadão brasileiro, nato ou naturalizado, será identificado em todas as suas relações com a sociedade e com os organismos governamentais e privados.*", e no artigo 2º "*É instituído o Cadastro Nacional de Registro de Identificação Civil, destinado a conter o número único de Registro Civil acompanhado dos dados de identificação de cada cidadão.*", teve como inspiração fatos que levaram ao impeachment de um presidente brasileiro, e que expuseram uma das fragilidades do sistema de identificação no Brasil, qual seja: Obedecendo ao princípio federativo, cada estado tem competência, delegada pela Lei 7116/83, para emitir carteiras de identidade que são, na sua esmagadora maioria, elaboradas a partir de certidões de nascimento ou casamento. Essas certidões são verificadas visualmente apenas, não sendo impossível sua adulteração ou falsificação. Como não há comunicação entre os estados, nada impede que uma pessoa obtenha documentos de identidade em distintos estados, com numerações diferentes (para não falar na possibilidade da adulteração da certidão original), o que dificulta a identificação. A regulamentação dessa lei, porém, demora até os dias de hoje, dadas as dificuldades materiais e políticas para se mudar a estrutura de identificação vigente, e os debates surgidos em função do número único do RIC. A introdução da Internet com sua posterior expansão para as áreas de finanças (home banking), comércio (eCommerce) e governo (eGov), no entanto se encarregou de tirar a Lei 9454 do limbo jurídico, já que passou a ser do interesse dos segmentos citados.

3.2. INSTITUTO NACIONAL DE IDENTIFICAÇÃO - INI

Como mencionamos, a estrutura de identificação consolidada no Brasil pela Lei 7116 está a cargo das autoridades policiais. Em cada um dos estados e no Distrito Federal, existe um Instituto de Identificação subordinado à Polícia Civil, por sua vez subordinada a uma Secretaria de Segurança. Essa Lei, regulamentada pelo Decreto 89250/83, estabeleceu também a obrigatoriedade de registros datiloscópicos dos cidadãos identificados. São coletadas e armazenadas em fichas as impressões digitais dos dez dedos das mãos, como forma de dirimir dúvidas quanto à identidade. Essas fichas fazem parte do acervo de cada um dos Institutos de Identificação estaduais. Com a implantação do SINIC – Sistema Nacional de Identificação Criminal - foi criado um cadastro centralizado no Instituto Nacional de

Identificação - INI, órgão vinculado à Polícia Federal e sediado em Brasília – DF, para onde devem ser encaminhadas as fichas datiloscópicas das pessoas identificadas criminalmente em qualquer dos 27 estados brasileiros. Esse cadastro é tratado por um sistema automatizado AFIS (Automated Fingerprint Identification System). O AFIS objeto desse estudo é um conjunto de hardware, software e bases de dados, que armazena e gerencia dados biográficos e criminais de indivíduos, associados a imagens digitalizadas de suas respectivas fichas datiloscópicas, permitindo que a pesquisa de espécimes – ou mesmo fragmentos – de impressões seja feita com eficiência e precisão. No caso, como detalharemos mais adiante, o objetivo do AFIS é de identificação, ou seja, fornecida uma impressão ou fragmento, o sistema procurará em todas as bases de dados impressões armazenadas que correspondam às características informadas, numa pesquisa (1:N), podendo retornar um resultado positivo, ou negativo, ou mais de um semelhante. É portanto diferente dos sistemas de verificação ou validação, onde se informa previamente quem é o suposto indivíduo e o sistema faz apenas uma pesquisa (1:1), retornando resultado ou positivo ou negativo. Há vários fornecedores desses sistemas atualmente, e um dos seus diferenciais é o algoritmo de classificação e pesquisa que utilizam: De toda forma, há padrões emitidos pelo ANSI (American National Standars Institute), NIST (National Institute of Standards and Technology) e FBI (Federal Bureau of Investigations), o grande cliente nos Estados Unidos [11].

3.3. INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS – ICP BRASIL

> *É um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.*
>
> *http://www.icpbrasil.gov.br/*

A Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil [4], foi instituída através da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, sendo o Instituto Nacional de Tecnologia da Informação - ITI, [12] autarquia federal vinculada à Casa Civil da Presidência da República, sua Autoridade Certificadora Raiz - AC Raiz.

Os documentos assinados eletronicamente utilizando Certificados Digitais emitidos por alguma entidade que seja credenciada à ICP-Brasil possuem validade jurídica, pois a Medida Provisória que a instituiu lhes garante a autenticidade e integridade necessárias,

conforme disposto em seu Artigo 10º, Parágrafo 1º. No entanto, o parágrafo 2º do mesmo artigo não veda a utilização de outros meios de comprovação de autoria e integridade.

Sua estrutura atual é:

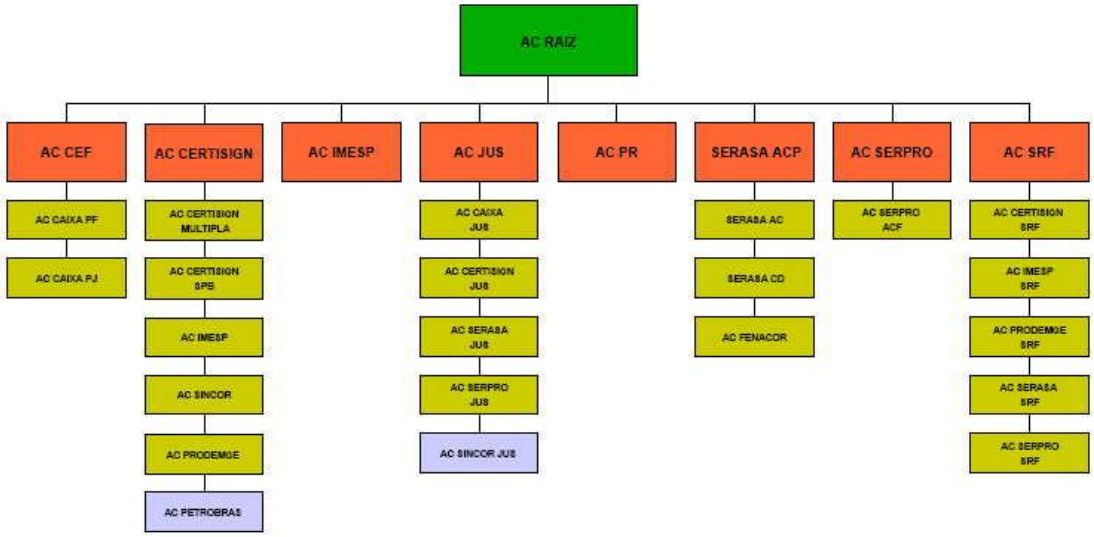

Figura 9: Estrutura da ICP-Brasil. Fonte: http://www.iti.br

As declarações de práticas e procedimentos estão descritos em http://www.iti.gov.br, notadamente no documento PADRŐES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL [13]. Os algoritmos utilizados, bem como sua estrutura de chaves e respectivas datas de validade, estão descritos no mesmo local, e demonstrados na figura a seguir:

	AUTORIDADE CERTIFICADORA RAIZ	AUTORIDADE CERTIFICADORA 2° NIVEL	USO DO CERTIFICADO FINAL AUTENTICAÇÃO	USO DO CERTIFICADO FINAL ASSINATURA
VERSÃO	V0			
ASSIMETRICO	RSA2048	RSA2048	RSA1024/2048	RSA1024/2048
HASH	SHA1	SHA1	SHA1	SHA1
DT INICIO	30/11/2001			
DT FIM	30/11/2011	30/10/2011	30/10/2011	31/12/2010
VERSÃO	V1			
ASSIMETRICO	RSA2048	RSA2048	RSA1024/2048/ECC	RSA1024/2048/ECC
HASH	SHA1	SHA1	SHA1/256/512/WHIR	SHA1/256/512/WHIR
DT INICIO	05/06/2008			
DT FIM	31/12/2013	31/12/2013	31/12/2013	31/12/2010
VERSÃO	V2A			
ASSIMETRICO	RSA4096	RSA4096	RSA2048/ECC	RSA2048/ECC
HASH	SHA512/WHIR	SHA512/WHIR	SHA256/512/WHIR	SHA256/512/WHIR
DT INICIO	31/12/2008			
DT FIM	31/12/2021	31/12/2021	31/12/2021	31/12/2021
VERSÃO	V2B			
ASSIMETRICO	ECC512	ECC512	ECC256/512	ECC256/512
HASH	SHA512/WHIR	SHA512/WHIR	SHA256/512/WHIR	SHA256/512/WHIR
DT INICIO	31/12/2009			
DT FIM	31/12/2022	31/12/2023	31/12/2023	31/12/2023

Figura 10: Algoritmos e chaves da ICP-Brasil. Fonte: http://www.iti.br

3.3.1. Autoridade Certificadora Raiz – AC-Raiz

No Brasil, a operação deste serviço utiliza a infra-estrutura do Serviço Federal de Processamento de Dados – SERPRO que, por sua vez, deve seguir as resoluções que regulamentam o credenciamento e operação das Autoridades Certificadoras no Brasil, divulgadas pelo ITI.

Devido à sua importância, o quesito Segurança é fundamental na manutenção de uma estrutura de Chaves Públicas, pois uma vez que esta seja comprometida, toda a hierarquia de Chaves estará condenada, sendo necessário revogar e re-emitir milhares de certificados digitais. Assim, faz-se necessária a execução de auditorias de conformidade periódicas para aferir se os requisitos de segurança estão sendo seguidos. Em janeiro de 2006 o SERPRO certificou seu Centro de Certificação Digital – CCD SERPRO, localizado no Rio de Janeiro, segundo a norma de segurança britânica BS 7799, atual ISO/IEC 27001:2006.

3.3.2. Autoridades Certificadoras – ACs

O Brasil conta com diversas ACs autorizadas a emitir estes certificados, podendo-se citar a Caixa Econômica (AC CEF), o SERPRO (AC SERPRO ACF) e Certisign (AC CERTISIGN) [18] e Secretaria da Receita Federal (AC SRF), dentre outras.

3.3.3. Autoridades de Registro – ARs

Podemos citar SERASA, Caixa Econômica Federal, Correios, Ordem dos Advogados do Brasil, entre outros.

3.4. DOCUMENTO DE IDENTIFICAÇÃO ÚNICO

O projeto brasileiro de um RIC – Registro de Identificação Civil será fortemente baseado no sistema AFIS do INI - Instituto Nacional de Identificação. O processo de coleta das impressões digitais seria o embrião do SINRIC – Sistema Nacional de Registro de Identificação Civil. A idéia é submeter as digitais coletadas do cidadão candidato ao documento ao sistema, para que seja verificada, em todo o cadastro já existente (pesquisa 1:N), a existência dessas digitais. Em caso negativo, o sistema atribuirá ao cidadão um número de identificação único para todo o território nacional, e prosseguirá no processo de elaboração do documento. Caso contrário, se trata de tentativa – provavelmente fraudulenta - de obter uma nova identidade.

Pela proposta atual, a solicitação do documento e a respectiva coleta de dados para sua elaboração caberiam aos Institutos de Identificação estaduais. O Instituto Nacional de Identificação seria o encarregado de operar o sistema e emitir o documento, que seria validado, como vimos, antes da emissão. A captura e posterior remessa dos dados ao INI pode ser on-line, por remessa em meio magnético ou por remessa de formulários em papel, tudo isso dependendo da disponibilidade de meios no local da coleta.

As metas divulgadas (Fagundes e Araújo, 2008) prevêem o início de um projeto piloto em janeiro de 2009. aproveitando parte da estrutura do SINIC – além do AFIS, estações de coleta, servidores web e de armazenamento, impressoras – visando atingir um público alvo de 2 milhões de cidadãos. Esse número seria ampliado em 2010 para 8 milhões de cidadãos. Em 2011 seriam emitidas 20 milhões de carteiras, com ampliação de capacidade para 80.000 aquisições/dia, e já cobrindo os 27 estados. Armazenamento também ampliado para 30 milhões. Objetivo final seria alcançado em 2017, com 150 milhões de documentos emitidos.

O custo estimado pelo Instituto Nacional de Identificação para todo o projeto seria de US$ 700.000.000, sendo que para ampliação do AFIS e implantação do sistema seriam gastos de US$ 250 a 300.000.000, o custo de emissão das carteiras seria, a preços de hoje, US$ 300.000.000. Se prevê a instalação de 4700 estações de coleta, US$ 30.000.000 seu custo aproximado [14].

O novo número seria gerado quando da primeira emissão do novo documento, que é estimada para os cidadãos com mais de dezesseis anos de idade.

O modelo proposto pelo Instituto Nacional de Identificação para o RIC se assemelha aos dos demais países europeus mencionados. Suas funções seriam identificar o cidadão presencial e remotamente. Teria como conteúdo visível foto, assinatura e a impressão digital de um dos indicadores. Teria também o identificador OCR padrão 9303 da ICAO (International Civil Aviation Organization, emite padrões para os MRTD – Machine Readable Travel Documents), que o habilitaria como documento internacional em viagens para países do Mercosul, por exemplo [15]. O conteúdo não-visível, gravado no chip, teria, entre outros, impressões digitais dos dez dedos, chaves privada e pública geradas quando de sua emissão, e certificado digital. Seu protótipo é como segue:

Figura 11: Proposta do INI. Fonte: Correio Braziliense 06/07/2008

3.5. PRINCIPAIS PROBLEMAS

Apesar da segurança e facilidades que estas ferramentas proporcionam, o alto custo de implantação para cidadãos comuns e pequenas empresas tem dificultado a plena difusão da prática do uso do Certificado Digital no dia-a-dia.

Complexidade da estrutura do Estado: Intervenção de diversos Ministérios, Estados da federação, Departamento de Polícia Federal, Polícias estaduais, Presidência da República, Banco Central, Tribunal Superior Eleitoral, Cartórios de Registro, entre outros com distintos graus de liberdade e de interesses, resultando em dificuldade de estabelecer padrões.

Complexidade da solução – Disponibilidade da infra-estrutura, alternativas de coleta e transmissão de dados num país com nossas características geográficas, políticas e sociais. A coleta para o sistema AFIS hoje é aplicada sobre universo de 2 por cento da população, e demanda intervenção humana especializada para dirimir casos de “falsos positivos” e “falsos negativos”.

Preocupações com a privacidade e o controle que o estado poderia exercer sobre o cidadão, em contraste com um aumento da segurança por identificar claramente os desonestos e dificultar suas ações.

4. CONCLUSÃO

Entendemos que a implantação, no Brasil, de um documento de identificação civil do cidadão mais seguro, que integre informações de diversas organizações e que estenda sua funcionalidade para a identificação remota, se trata de processo irreversível, apoiado em interesses econômicos extremamente fortes. Por um lado a Febraban, entidade que congrega os bancos comerciais, mesmo sem divulgar dados referentes a perdas, revela que, só em 2007, foram investidos R$ 1,7 bilhão(!) pelos bancos brasileiros apenas no quesito segurança eletrônica, aí incluído o desenvolvimento de sistemas de detecção de fraudes, monitoramento intensivo e prejuízos com fraudes diversas envolvendo identidades (Higashino, 2008) [16]. Por outro, o INSS perde algo como R$ 10 bilhões(!) por ano no pagamento de benefícios fraudulentos (Pimentel, 2008) [17]. Causa primária: A má qualidade dos atuais documentos de identificação brasileiros. Acrescente-se a isso o movimento dos fornecedores de soluções de identificação, que se organizaram na ABRID - Associação Brasileira das Empresas de Tecnologia em Identificação Digital (www.abrid.org.br).

Vemos no entanto obstáculos para transformação desse novo documento em documento único, ou mesmo documento de cidadania plena: A grande quantidade de atores envolvidos no processo, com suas estruturas próprias e redundantes, alicerçadas na divisão do Estado entre 3 poderes distintos e no pacto federativo, nos parece a principal. Não vimos estudos de integração ou interoperabilidade com o voto eletrônico, por exemplo, que poderia ser um “certificado de atributo” do documento principal. Ao contrário, seus gestores fazem estudos e projetos independentes. O mesmo acontece com documentos como a carteira nacional de habilitação.

Quanto ao quesito segurança, se trata inegavelmente de um gigantesco progresso, pela virtual impossibilidade de um mesmo conjunto de impressões digitais gerar mais de um número único de identificação. Apesar do documento base para a identificação, como as certidões de nascimento e casamento, continuar inalterado, e de haver outros documentos que têm fé pública, acreditamos que ao final do ciclo de vida das atuais carteiras de identidade as perdas com fraudes associadas tendam a zero.

5. PRINCIPAIS PADRÕES

ECC *Eliptic Curve Cryptography*, é uma variante da criptografia assimétrica ou de chave pública, baseada na matemática das curvas elípticas

International Common Criteria é um padrão internacional (ISO/IEC 15408) para segurança da computação. O Common Criteria assegura que o processo de especificação, implementação e avaliação de um produto para segurança da computação foi conduzido de maneira padronizada e rigorosa. O **Evaluation Assurance Level** (**EAL1** a **EAL7**) de um produto de TI ou sistema é um grau numérico ascendente atribuído após testes, e assegura que os princípios de segurança inerentes foram implementados.

EMV é um padrão de interoperabilidade dos smart cards e respectivos terminais de leitura, para autenticação de cartões de débito e crédito. O nome vem das iniciais de Europay, MasterCard e VISA, as três companhias que colaboraram para o desenvolvimento desse padrão, fortemente baseado na ISO 7816, que define a interface do ICC (cartão com circuitos integrados).

- Tecnologias básicas e Padrões do cartão utilizado em Portugal (Gemalto, 2008):

Cartão:

ISO/IEC 9798 (device-authentication/Secure messaging);
ISO 7810;
ISO 7811;
ISO 7811;
ISO 7816;
ISO 10373;
ISO/IEC 10373;
EN 742:1993;
CECC 90000;
MI STD-883C;
Pr CEN/TS 15480 1,2 (European Citizen Card - draft);
ICAO 9303 (travel documents);

Chip:

ISO/IEC 7810
ISO 7816;
ISO/IEC 14443;

Java Card/GP (suporte de Java cards, ISO/IEC 7501-3 (ICAO))

CEN / TC 2254;

CWA 15264;

CWA 14890;

ISO/IEC 19794-2: Finger Minutiae data;

ISO/IEC 19794-4,5 : Finger Image data;

ISO/IEC 19784 – BioAPI;

ISO/IEC 19785 – CBEFF;

ISO/IEC 24727

EMV

Biometria:

ISO/IEC/JTC 1 SC 37;

ISO/IEC 7816-11;

ISO/IEC FCD 19794-2 (fingerprint minutiae);

ISO/IEC 19784-1 BioAPI;

ISO/IEC 19785-1 Common Biometric Exchange formats (CBEFF) - Part 1: Data Element Specification.

PKI, Certificados e Assinaturas Digitais:

ISO/IEC 7816-15;

CWA 14890 - CEN/ISSS Workshop on the electronic signature (Area K);

CWA 15264 (eAuthentication);

CWA 14167 (Mutipart);

PKCS#1, PKCS#3 , PKCS#7, PKCS#8, PKCS#10, PKCS#11, PKCS#12, PKCS#15.

BIBLIOGRAFIA

[1] “Projecto Cartão do Cidadão” Disponível em **http://www.cartaodecidadao.pt/** . Acesso em 15 de janeiro de 2008.

[2] Ferreira, Aurélio B. de Holanda. Novo Dicionário da Língua Portuguesa. 1. ed. Rio de Janeiro, Nova Fronteira, 1975

[3] LEI Nº 7.116, de 29 de Agosto de 1983, DECRETO Nº 89.250, de 27 de Dezembro de 1983. Disponíveis em http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=128295 e http://www.planalto.gov.br/ccivil_03/decreto/D89250.htm . Acesso em 27de Outubro de 2007.

[4] ICP-Brasil: Infra-estrutura de Chaves Públicas Brasileiras. Disponível em **http://www.icpbrasil.gov.br** . Acesso em 04 de Setembro de 2006.

[5] LEI Nº 9454, de 7 de Abril de 1997. Disponível em http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=145939 e http://www.planalto.gov.br/ccivil_03/Leis/L9454.htm. Acesso em 27 de Outubro de 2007.

[6] Java Card Platform Specification 2.2.1 – Sun Microsystems. Disponível em http://java.sun.com/javacard/specs.html Acesso em 27 de Outubro de 2007.

[7] Relatório de Melhores Práticas Mundiais – UCMA – Unidade de Coordenação da Modernização Administrativa. Disponível em http://www.cartaodocidadao.pt/images/stories/melhores_praticas_internacionais.pdf Acesso em 15 de janeiro de 2008.

AMA – Agência para a Modernização Administrativa, em http://www.ama.pt/ http://www.portaldocidadao.pt/PORTAL/pt/Dossiers/DOS_cartao+de+cidadao+_+o+novo+documento+de+cidadania.htm?passo=6 . Acesso em 02 de Julho de 2007.

[8] Gallo, Enrique Vázquez e Ávila, Carmen Sanchez - Sistemas Nacionales de Identificación Electrônica en el Entorno Europeo y Norteamericano. Disponível em http://www.madrimasd.org/tic/Informes/Downloads_GetFile.aspx?id=6089 Acesso em 15 de janeiro de 2008.

[9] Eched, Youval et al. - e-Government 2.0 Identification, Security and Trust. Disponível em http://www.gemalto.com/public_sector/e-gov.html Acesso em 14 de Julho de 2008.

[10] http://www.gemalto.com/companyinfo/smart_cards_basics/ Acesso em 14 de Julho de 2008.

[11] AFIS: http://en.wikipedia.org/wiki/Automated_fingerprint_identification_system

[12] Instituto Nacional de Tecnologia da Informação. Disponível em **http://www.iti.br** . Acesso em 04 de setembro de 2006.

[13] PADRŐES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL Acesso em 27 de Outubro de 2007: DOC_ICP_01_01_v1_0.pdf

[14] Fagundes, Paulo Roberto e Araújo, Marcos Elias – INI (Instituto Nacional de Identificação) – Encontro Nacional de Identificação, Brasília 09 de Julho de 2008

[15] ICAO International Civil Aviation Organization – Padrão 9303 – MRTD http://www2.icao.int/en/mrtd/Pages/default.aspx - Acesso em 28 de Setembro de 2007.

[16] Higashino, Jorge – Febraban – Encontro Nacional de Identificação, Brasília 09 de Julho de 2008 - http://www.febraban.org.br/

[17] Pimentel, José – INSS – Encontro Nacional de Identificação, Brasília 10 de Julho de 2008 - Boletim Estatístico da Previdência Social: Disponível em http://www.mpas.gov.br/pg_secundarias/previdencia_social_13_05.asp -

[18] http://www.iti.gov.br/twiki/bin/view/Certificacao/PerguntasFrequentes e CERTISIGN: Autoridade Certificadora (AC) que obedece à estrutura da ICP-Brasil. Disponível em **http://www.certisign.com.br** Acesso em 04 de setembro de 2006.

- DAMATTA, Roberto . A Mão Visível do Estado: Notas para o Significado Cultural dos Documentos na Sociedade Brasileira. Anuário Antropológico, n. 99, p. 37-64, 2002, Ed. Tempo Brasileiro.

- ALECRIM, Emerson. Assinatura digital e Certificação digital. Artigo publicado em 25/09/2005. Disponível em **http://www.infowester.com/assincertdigita.php.** Acesso em 04 de setembro de 2006.

- KUHN, D. Richard et a. Introduction to Public Key Technology and the Federal PKI Infrastructure. Disponível em **http://www.modulo.com.br/pdf/de010226-pki.pdf.** Acesso em 04 de setembro de 2006.

http://www.microsoft.com/brasil/setorpublico/temas/certificacao.mspx Pro-Uni, Projeto CERES (Espanha). Acesso em 02 de Julho de 2007.

Freitas, Christiana Soares de e Veronese, Alexandre. “Segredo e Democracia: certificação digital e software livre” – Revista iP – Informática Pública, Nº 2 MAIO 2007

Martini, Renato. Criptografia e Cidadania Digital . Rio de Janeiro, editora Ciência Moderna, 2001, e em http://www.iti.br/twiki/bin/view/Midia/MidiaClip2007jun19 Acesso em 04 de Julho de 2007.

Rezende, Pedro Antonio Dourado de. Disponível em http://www.cic.unb.br/docentes/rezende/trabs/jcsbc22.htm Acesso em 04 de Julho de 2007.

Barra, Marcelo. Dissertação de mestrado, defendida e aprovada em 08/2007 no Instituto de Ciências Sociais da Universidade de Brasília. Revista iP – Informática Pública Nº 2 MAIO 2007